(odtis vzglavne štampiljke)

ZAPISNIK

o preiskavi elektronske naprave

(8. odstavek 219.a člena Zakona o kazenskem postopku)

30. 1. 2014 je bil v kraju Zgornji Dol, Uradniška cesta 5, opravljen postopek preiskave elektronske naprave. Preiskava se opravi na osnovi izdane odredbe za preiskavo elektronske naprave Okrožnega sodišča v Zgornjem Dolu, št. XI/1000, z dne 14. 1. 2014, ki je bila vročena Dejanu Nepridipravu, dne 26. 1. 2014. Elektronska naprava je bila 4. 1. 2014 na osnovi zapisnika o zasegu predmetov zasežena imetniku Dejanu Nepridipravu, rojenemu 1. 2. 1985, stanujočemu na Počitniški ulici 10 v Zgornjem Dolu. 28. 1. 2014 je bilo opravljeno zavarovanje podatkov elektronske naprave, o čemer je bil napisan zapisnik o zavarovanju podatkov elektronske naprave.

Preiskavo elektronske naprave je opravil:

- Bojan Preiskovalec iz Policijske uprave Zgornji Dol.

Pri preiskavi ni bilo sodelujočih in navzočih oseb. Preiskava se je začela 30. 1. 2014 ob 8.10.

I. NAMEN PREISKAVE

Zavarovane elektronske podatke (istovetno kopijo) je treba preiskati z namenom, da bi se odkrili sledovi in pridobili dokazi, ki bi potrdili sum storitve kaznivega dejanja prikazovanja, izdelave, posesti in posredovanja pornografskega gradiva po 176/III. členu KZ-1, ter podatki, na osnovi katerih bi lahko identificirali in odkrili osumljenca navedenega kaznivega dejanja.

II. IDENTIFIKACIJA PREISKOVANIH NOSILCEV PODATKOV

Preiskujejo se zavarovani podatki (istovetna kopija) USB-podatkovnega nosilca znamke Transcend, model JetFlash V30, s serijsko številko D33193, črne barve, deklarirane kapacitete 8 GB.

III. NAČIN IZVEDBE PREISKAVE

Sliko podatkov iz navedenega USB-podatkovnega nosilca (sklop treh datotek od *Transcend_8GB_USB.E01* do *Transcend_8GB_USB.E03*) priključim v program AccessData FTK

Imager, različice 3.0.1.1467, s katerim preverim integriteto podatkov. Z navedenim programom izračunam zgoščeni vrednosti MD5 in SHA-1 vhodnih podatkov, pri tem pa ugotovim, da se zgoščeni vrednosti MD5 (661d185741c8dc11b221b62ebaf4f0fd) in SHA-1 (07bf9aa6c8a182a8eff532ce76b6a72a1ce8a63e) slike podatkov ujemata z zgoščenima vrednostma MD5 in SHA-1, ki sta bili izračunani pri postopku zavarovanja podatkov (razvidno iz zapisnika o zavarovanju podatkov elektronske naprave). Na osnovi ujemanja zgoščenih vrednosti podatkov je možno potrditi integriteto slike podatkov, ki se bodo preiskovali v nadaljevanju.

Nadaljnji postopki so opravljeni s programom za izvajanje digitalne forenzike X-Ways Forensics, različice 16.7 SR-9. Na namenski delovni postaji ustvarim imenik za izločene podatke *transcend_usb**podatki* in imenik za elektronska poročila *transcend_usb**poročila*. Pri vpogledu v strukturo preiskovanega podatkovnega nosilca ugotovim, da je na njem ena diskovna particija velikosti ~7,5 GB, z datotečnim sistemom FAT32, imenom nosilca »Izmenjava« in serijskimi številkami nosilca »53D2-9D42«. Za vse datotečne objekte na predmetnem podatkovnem nosilcu izračunam zgoščeno vrednost MD5, nato pa izdelam seznam vseh datotek (vključno z datotečno strukturo in metapodatki datotečnih objektov), ki ga shranim v datoteko *transcend_usb**poročila**seznam_datotek.txt*.

Pri vpogledu v datotečno strukturo ugotovim, da je na preiskovanem podatkovnem nosilcu pet grafičnih datotek, ki so imenovane *pt_picture-1.jpg*, *pt_picture-2.jpg, pt_picture-3.jpg, pt_picture-4.jpg* in *pt_picture-5.jpg*. Pri vsebinskem pregledu navedenih datotek ugotovim, da slikovne datoteke prikazujejo spolne zlorabe otrok. Iz metapodatkov datotečnega sistema je razvidno, da so vse navedene datoteke v okviru datotečnega sistema nastale 24. 7. 2013 ob 13.44, da so bile zadnjič spremenjene 24. 7. 2013 ob 13.48 in da je 4. 1. 2014 zadnji shranjen čas dostopa do njih. Podrobnosti so razvidne iz predhodno ustvarjenega seznama vseh datotek (*transcend_usb**poročila* *seznam_datotek.txt*). V nadaljevanju opravim analizo t. i. Exif metapodatkov slikovnih datotek, pri tem pa ugotovim, da vse navedene grafične datoteke vsebujejo zgolj naslednje metapodatke: izdelovalec naprave »Casio«, model naprave »QV-4000«, ločljivost slike »2240 x 1680«. Vse navedene datoteke izločim v imenik *transcend_usb**podatki*, pri tem pa ohranim prvotna imena datotek.

Z uporabo orodja X-Ways Forensics v nadaljevanju izvedem postopek temeljitega priklica vseh predhodno izbrisanih datotečnih objektov. Pri tem je bilo identificiranih dodatnih 18 datotek različnih tipov. Nato izvedem postopek iskanja na osnovi unikatnega podpisa bolj

razširjenih formatov datotek. Pri tem je bilo identificiranih dodatnih 23 datotek različnih tipov. Za vse novo identificirane datoteke izračunam zgoščeno vrednost MD5, nato pa izdelam nov seznam vseh obstoječih in dodatno identificiranih datotek (vključno z datotečno strukturo in metapodatki datotečnih objektov), ki ga shranim v datoteko *\transcend_usb\poročila\seznam_datotek _razširjen.txt*.

Predhodno izračunane zgoščene vrednosti MD5 vseh identificiranih datotek primerjam z zgoščenimi vrednostmi MD5 iz zbirke t. i. »slabih« datotek, za katere je bilo že v predhodnih postopkih ugotovljeno, da vsebujejo sporne vsebine. Pri tem ugotovim, da med preiskovanimi podatki ni nobene datoteke, ki bi bila v predhodnih postopkih že opredeljena kot sporna vsebina.

Dodatno identificirane grafične datoteke vsebinsko pregledam, pri tem pa ugotovim, da so v treh datotekah (*pt_picture-7.jpg*, *pt_picture-8.jpg* in *pt_picture-9.jpg*) vsebine, ki prikazujejo spolno zlorabo otrok. Iz metapodatkov datotečnega sistema je razvidno, da so vse navedene datoteke v okviru datotečnega sistema nastale 24. 7. 2013 ob 13.44, da so bile zadnjič spremenjene 24. 7. 2013 ob 13.48 in da je 29. 8. 2013 zadnji shranjen čas dostopa do njih. Podrobnosti so razvidne iz predhodno ustvarjenega seznama vseh datotek (*\transcend_usb\poročila\seznam_datotek_razširjen.txt*). V nadaljevanju opravim analizo t. i. Exif metapodatkov slikovnih datotek, pri tem pa ugotovim, da vse navedene grafične datoteke vsebujejo zgolj naslednje metapodatke: izdelovalec naprave »Casio«, model naprave »QV-4000«, ločljivost slike »2240 x 1680«. Vse navedene datoteke izločim v imenik *\transcend_usb\podatki*, pri tem pa ohranim prvotna imena datotek.

Pri vsebinskem pregledu dodatno identificiranih grafičnih datotek se osredotočim na datoteko *DSC_0023.jpg*, ki prikazuje osebno vozilo znamke Fiat, model Punto, rdeče barve, z nameščeno zadnjo registrsko tablico s številko ZD 25-46K. Prav tako se osredotočim na datoteko *DSC_0024.jpg*, ki prikazuje notranjost osebnega vozila znamke Fiat, model Punto, v katerem na voznikovem sedežu sedi neznana moška oseba. Nato opravim analizo t. i. Exif metapodatkov obeh slikovnih datotek, pri tem pa ugotovim, da vse navedene grafične datoteke vsebujejo zgolj naslednje metapodatke: izdelovalec naprave »Casio«, model naprave »QV-4000«, ločljivost slike »2240 x 1680«. Iz metapodatkov datotečnega sistema je razvidno, da sta obe navedeni datoteki v okviru datotečnega sistema nastali 27. 7. 2013 ob 17.24, da sta bili zadnjič spremenjeni 27. 7. 2013 ob 17.24 in da je 29. 8. 2013 zadnji shranjen čas dostopa do njih. Podrobnosti so razvidne iz predhodno ustvarjenega seznama vseh datotek (*\transcend_usb\poročila\seznam_datotek_razširjen.txt*). Obe navedeni

datoteki izločim v imenik *transcend_usb**podatki*, pri tem pa ohranim prvotni imeni datotek.

Med dodatno identificiranimi datotekami je tudi datoteka *Življenjepis.doc*, za katero opravim podrobnejšo analizo. Pri tem ugotovim, da so med vsebino med drugim tudi ime in priimek »Dejan Nepridiprav« ter naslov »Počitniška ulica 10, Zgornji Dol«. Pri analizi metapodatkov navedene datoteke je bilo ugotovljeno, da je bila ustvarjena na računalniku z dodeljenim imenom »Učilnica14« in da je avtor dokumenta uporabnik »Učilnica14\DNepridiprav«. Iz metapodatkov datotečnega sistema je razvidno, da je navedena datoteka v okviru datotečnega sistema nastala 29. 8. 2013 ob 9.04, da je bila zadnjič spremenjena 30. 8. 2013 ob 11.17 in da je 2. 9. 2013 zadnji shranjen čas dostopa do nje. Podrobnosti so razvidne iz predhodno ustvarjenega seznama vseh datotek (*transcend_usb**poročila**seznam_datotek_razširjen.txt*). Navedeno datoteko izločim v imenik *transcend_usb**podatki*, pri tem pa ohranim prvotno ime datoteke.

Nato izvedem iskanje unikatnih iskalnih nizov med surovimi podatki, in sicer »Casio« in »QV-4000«. Pri tem sem med preiskovanimi podatki našel 11 iskalnih zadetkov za oba unikatna iskalna niza. Pri nadaljnji analizi je bilo ugotovljeno, da deset iskalnih zadetkov pripada podatkom v okviru predhodno navedenih grafičnih datotek (*pt_picture-1.jpg*, *pt_picture-2.jpg*, *pt_picture-3.jpg*, *pt_picture-4.jpg*, *pt_picture-5.jpg*, *pt_picture-7.jpg*, *pt_picture-8.jpg*, *pt_picture-9.jpg*, *DSC_0023.jpg* in *DSC_0024.jpg*). Enajsti iskalni zadetek pa pripada segmentu podatkov s poškodovanim unikatnim podpisom grafične datoteke formata *JPG*. Med segmenti podatkov so namreč razvidni zgolj t. i. Exif metapodatki, medtem ko je bila druga vsebina predhodno že prepisana z drugimi podatki.

V nadaljevanju opravim analizo vseh preostalih identificiranih datotek in drugih podatkov, vendar pri tem ne najdem za zadevo relevantnih vsebin. Drugih posebnosti pri preiskavi elektronske naprave nisem ugotovil.

Vse datoteke, ki so bile izločene oziroma ustvarjene v nadrejenih imenikih *transcend_usb**podatki* in *transcend_usb**poročila*, so bile z uporabo programa 7-Zip, različice 9.20, stisnjene v arhivsko datoteko *transcend_usb_izločeno.zip*. Z uporabo programa AccessData FTK Imager, različice 3.0.1.1467, sem nato za navedeno datoteko izračunal zgoščeni vrednosti MD5 (c434b74a34829f25c0190d05b6f23f74) in SHA-1 (8f84f5a9918e500816115a0b15502702410ac4c7), s katerima se zagotavlja integriteta pri preiskavi izločenih podatkov.

Sliko podatkov iz preiskovanega USB-podatkovnega nosilca (sklop treh datotek od *Transcend_8GB_USB.E01* do *Transcend_8GB_USB.E03*) priključim v program AccessData FTK Imager, različice 3.0.1.1467, s katerim preverim integriteto podatkov. Z navedenim programom izračunam zgoščeni vrednosti MD5 in SHA-1 vhodnih podatkov, pri tem pa ugotovim, da se zgoščeni vrednosti MD5 (661d185741c8dc11b221b62ebaf4f0fd) in SHA-1 (07bf9aa6c8a182a8eff532ce76b6a72a1ce8a63e) slike podatkov ujemata z zgoščenima vrednostima MD5 in SHA-1, ki sta bili izračunani pri postopku zavarovanja podatkov (razvidno iz zapisnika o zavarovanju podatkov elektronske naprave). Na osnovi ujemanja zgoščenih vrednosti podatkov je možno potrditi integriteto slike podatkov, ki je bila preiskovana.

IV. UGOTOVITVE PREISKAVE

Pri preiskavi je bilo najdenih osem grafičnih datotek, ki prikazujejo spolne zlorabe otrok. Najdena je bila tudi ena grafična datoteka, iz katere je razvidno osebno vozilo znamke Fiat, model Punto, rdeče barve, z nameščeno zadnjo registrsko tablico s številko ZD 25-46K, in ena grafična datoteka, iz katere je razvidna notranjost vozila in neznana moška oseba na voznikovem sedežu. Vse navedene grafične datoteke imajo enake Exif metapodatke (izdelovalec »Casio«, model »QV-4000«, ločljivost »2240 x 1680«), medtem ko so datotečni metapodatki razvidni iz ustvarjenega seznama vseh datotek. V okviru datoteke *Življenjepis.doc* so bili najdeni tudi ime, priimek in naslov: »Dejan Nepridiprav«, »Počitniška ulica 10, Zgornji Dol«, ter metapodatki o imenu računalnika: »Učilnica14« in avtorju »Učilnica14\DNepridiprav«.

V. DRUGE POMEMBNE OKOLIŠČINE

Arhivska datoteka *transcend_usb_izločeno.zip* je bila shranjena na DVD-optični podatkovni nosilec na način, ki zagotavlja istovetnost in integriteto podatkov. Pri snemanju podatkov je bila izbrana tudi možnost zaprtja seje (angl. close session), kar onemogoča poznejše spreminjanje podatkov na optičnem podatkovnem nosilcu.

Preiskava je bila končana 30. 1. 2014 ob 12:35, zapisnik pa 30. 1. 2014 ob 13:45.

POLICIST:
Bojan Preiskovalec